IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Edward W. Kohler, Jr., et al.	Art Unit	: 2155
Serial No.	: 09/931,487	Examiner	: Shawki Saif Ismail
Filed	: August 16, 2001	Conf. No.	: 3664
Title	: THWARTING SOURCE ADDRESS SPOOFING-BASED DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF EDWARD W. KOHLER, JR., ET AL

Please charge the Appeal Brief fee of $250 to Deposit Account No. 06-1050. Please apply any other charges or credits to Deposit Account No. 06-1050.

(i.) Real Party In Interest

The real party in interest in the above application is Mazu Networks, Inc.

(ii.) Related Appeals and Interferences

The appellant is not aware of any appeals or interferences related to the above-identified patent application.

(iii.) Status of Claims

This is an appeal from the decision of the Primary Examiner in a Final Office Action dated June 14, 2006 rejecting claims 1-33 all of the claims in the application. The claims have been twice rejected. Claims 1-33 are the subject of this appeal.

(iv.) Status of Amendments

Claim amendments filed on September 1, 2006 were not entered.[1] The examiner considered that this amendment required further consideration and/or search, which in Appellant's opinion is unfortunate, since it would have clarified issues on appeal. Appellant argues the claims without the un-entered amendment, but will note for the Board the discrepancies and correct language, which will be provided by amendment when the case is allowed.

Appellant filed a Notice of Appeal on December 14, 2006.

(v.) Summary of Claimed Subject Matter

Background

The invention relates to techniques to thwart network-related denial of service attacks. In denial of service attacks, an attacker sends a large volume of malicious traffic to a victim in an attempt to prevent the victim from responding to legitimate traffic.

---

[1] Appellant filed Reply to the final action, which attempted to clarify language in claims 2-5, and 10 that would have removed the word victim. Victim does not presently find support in base claim 1. The amendment would have merely referred to "victim destination address" as "destination address for the data center," and the "victim data center" or "data center victim" as the "data center."

Appellant's Invention

Claim 1

One aspect of Appellant's invention is set out in claim 1, as a method of protecting a data center against a denial of service attack. "Referring to FIG. 1, an arrangement 10 to thwart denial of service attacks (DoS attacks) is shown." [Specification page 4, lines 27-28]

Inventive features of claim 1 include sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, "The data collectors 28 are located inter alia at major peering points and network points of presence (PoPs). The data collectors 28 sample packet traffic, accumulate, and collect statistical information about network flows." [Specification page 5, line 32 to page 6 line 4] the queries to request the statistical information from at least some of the data collectors. "The control center queries data collectors 28 and asks which data collectors 28 are seeing suspicious traffic being sent to the victim 12." [Specification page 12, lines 16-18].

Inventive features of claim 1 also include sending the statistical information from the data collectors in response to the queries. "Alternatively, the data collector can respond to queries concerning characteristics of traffic on the network. Typically, the queries can be for information pertaining to statistics." [Specification page 9, line 32 to page 10, line 3].

Inventive features of claim 1 also include processing the statistical information to determine the source of suspicious network traffic sent to the data center. "The packets from the attacker will have faked source addresses that will be changing with time. However, the control center can issue a query for this kind of packet by victim destination address. The data collectors 28 reply with the information collected. Based on that collected information from the data collectors 28, the control center can then determine what data centers are performing the spoofing on the victim 12." [Specification page 12, lines 19-26].

Claim 15

Claim 15 claims a method of protecting a victim data center against a denial of service attack. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 15 include receiving packets with faked, random source addresses. "The packets from the attacker will have faked source addresses that will be changing with time." [Specification page 12, lines 19-20].

Inventive features of claim 15 also include receiving, from a gateway disposed near the victim data center, a notification that the victim data center is under an attack. "The gateway 26 at the victim 12 contacts the control center and notifies the control center 24 that the victim 12 data center is under a spoofing attack." [Specification page 12, lines 8-10].

Inventive features of claim 15 also include sending queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network packets and collect statistical information on network packets sent over the network, the queries being requests for statistical information from data collectors that have examined network traffic with the victim destination address. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 15 also include determining the data center or centers involved in the attack on the victim data center by analyzing collected statistical information from the data collectors. This feature generally finds support at least as the analogous feature of claim 1.

Claim 20

Claim 20 claims a system to thwart denial of service attacks on a victim data center. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 20 include a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic. This feature generally finds support at least as the analogous feature of claim 1 and by "Gateways 26 and data collectors 28 are types of monitors that monitor and collect statistics on network traffic." [Specification page 5, lines 24-26].

Inventive features of claim 21 also include a control center coupled to the plurality of data collectors, the control center executing a computer program product stored on a computer readable medium. "The arrangement 10 to protect the victim includes a control center 24 that

communicates with and controls gateways 26 and data collectors 28 disposed in the network 14." [Specification page 5, lines 17-20].

Inventive features of claim 21 also include instructions to receive from the victim site a notification that the victim data center is under an attack. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 21 also include instructions to send queries to data collectors to request the statistical information from the data collectors, the statistical information used to determine the source of suspicious network traffic being sent to the victim. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 21 also include a gateway device that passes network packets between the network and the victim data center, the gateway disposed to protect the victim data center, and being coupled to the control center. "The gateway 26 devices are located at the edges of the Internet 14, for instance, at the entry points of data centers. The gateway devices constantly analyze traffic, looking for congestion or traffic levels that indicate the onset of a DoS attack." [Specification page 5, lines 28-32].

Claim 29

Claim 29 is directed to a computer program product residing on a computer readable media for protecting a victim data center against a denial of service attack. "The control center executes a computer program product stored on a computer readable medium." [Specification page 2, lines 23-24].

Inventive features of claim 29 include instructions to receive a notification that the victim data center is under an attack. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 29 also include instructions to send queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network traffic and collect statistical information on packets sent over the network, the queries to request statistical information from data collectors that have examined network traffic with the victim destination address. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 29 also include instructions to determine a source of the attack on the victim data center by analyzing collected information from the data collectors. This feature generally finds support at least as the analogous feature of claim 1.

(vi.) Grounds of Rejection to be Reviewed on Appeal

1. Claims 1-12 and 15-33 stand rejected under 35 U.S.C. 102(e), as being anticipated by Yavatkar et al., (Yavatkar) U.S. Patent No. 6,735,702.

2. Claims 13 and 14 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al., '702 in view of Hill et al., (Hill) U.S. Pat No. 6,088,804.

(vii.) Argument

Anticipation

"It is well settled that anticipation under 35 U.S.C. §102 requires the presence in a single reference of all of the elements of a claimed invention." *Ex parte Chopra*, 229 U.S.P.Q. 230, 231 (BPA&I 1985) and cases cited.

"Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

"This court has repeatedly stated that the defense of lack of novelty (i.e., 'anticipation') can only be established by a single prior art reference which discloses each and every element of the claimed invention." *Structural Rubber Prod. Co. v. Park Rubber Co.*, 223 U.S.P.Q. 1264, 1270 (Fed. Cir. 1984), citing five prior Federal Circuit decisions since 1983 including *Connell*.

In a later analogous case the Court of Appeals for the Federal Circuit again applied this rule in reversing a denial of a motion for judgment n.o.v. after a jury finding that claims were anticipated. *Jamesbury Corp. v. Litton Industrial Prod., Inc.*, 225 U.S.P.Q. 253 (Fed. Cir. 1985).

After quoting from *Connell*, "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim," 225 U.S.P.Q. at 256, the court observed that the patentee accomplished a constant tight contact in a ball valve by a lip on the seal or ring which interferes with the placement of the ball. The lip protruded into the

area where the ball will be placed and was thus deflected after the ball was assembled into the valve. Because of this constant pressure, the patented valve was described as providing a particularly good seal when regulating a low pressure stream. The court quoted with approval from a 1967 Court of Claims decision adopting the opinion of then Commissioner and later Judge Donald E. Lane:

> [T]he term "engaging the ball" recited in claims 7 and 8 means that the lip contacts the ball with sufficient force to provide a fluid tight seal **** The Saunders flange or lip only sealingly engages the ball 1 on the upstream side when the fluid pressure forces the lip against the ball and never sealingly engages the ball on the downstream side because there is no fluid pressure there to force the lip against the ball. The Saunders sealing ring provides a compression type of seal which depends upon the ball pressing into the material of the ring. *** The seal of Saunders depends primarily on the contact between the ball and the body of the sealing ring, and the flange or lip sealingly contacts the ball on the upstream side when the fluid pressure increases. 225 U.S.P.Q. at 258.

Relying on *Jamesbury*, the ITC said, "Anticipation requires looking at a reference, and comparing the disclosure of the reference with the claims of the patent in suit. A claimed device is anticipated if a single prior art reference discloses all the elements of the claimed invention as arranged in the claim." *In re Certain Floppy Disk Drives and Components Thereof*, 227 U.S.P.Q. 982, 985 (U.S. ITC 1985).

Obviousness

"It is well established that the burden is on the PTO to establish a prima facie showing of obviousness, *In re Fritsch*, 972 F.2d. 1260, 23 U.S.P.Q.2d 1780 (C.C.P.A., 1972)."

"It is well established that there must be some logical reason apparent from the evidence or record to justify combination or modification of references. *In re Regal*, 526 F.2d 1399 188, U.S.P.Q.2d 136 (C.C.P.A. 1975). In addition, even if all of the elements of claims are disclosed in various prior art references, the claimed invention taken as a whole cannot be said to be obvious without some reason given in the prior art why one of ordinary skill in the art would have been prompted to combine the teachings of the references to arrive at the claimed invention.

Id. Even if the cited references show the various elements suggested by the Examiner in order to support a conclusion that it would have been obvious to combine the cited references, the references must either expressly or impliedly suggest the claimed combination or the Examiner must present a convincing line of reasoning as to why one skilled in the art would have found the claimed invention obvious in light of the teachings of the references. *Ex Parte Clapp*, 227 U.S.P.Q.2d 972, 973 (Board. Pat. App. & Inf. 985)."

"The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon*, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984).

> Although the Commissioner suggests that [the structure in the primary prior art reference] could readily be modified to form the [claimed] structure, "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Laskowski*, 10 U.S.P.Q. 2d 1397, 1398 (Fed. Cir. 1989).

"The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination." *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 488 (Fed. Cir. 1984).

> Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under Section 103, teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) (emphasis in original, footnotes omitted).

"The critical inquiry is whether 'there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" *Fromson v. Advance Offset Plate, Inc.*, 225 U.S.P.Q. 26, 31 (Fed. Cir. 1985).

1. Yavatkar fails to anticipate Claims 1-12 and 15-33.

Claims 1, 7, 8 and 10-14

For the purposes of this appeal only, Claims 1, 7, 8 and 10-14 stand or fall together. Claim 1 is representative of this group of claims.

Claim 1 is directed to a method of protecting a data center against a denial of service attack. One of the advantages of Appellant's disclosed and claimed invention is that it is operable to detect and stop attacks (known, as well as, new attacks)[2], whereas, Yavatkar is only directed to finding a source of an attack, once the watchdog agent is notified that the data center is under attack.[3]

Claim 1 is neither anticipated nor obvious over Yavatkar, since Yavatkar neither describes nor suggests at least the features of … sending queries to data collectors, deployed at different points in a network … the queries to request the statistical information from at least some of the data collectors… and processing the statistical information to determine the source of suspicious network traffic sent to the data center.

The examiner contends that Yavatkar teaches the sending feature at (col. 3 line 65 - col. 4, line 23) and processing the statistical information to determine the source of suspicious network traffic sent to the data center at col. 3, lines 25-37 and col. 18, lines 32-53, in which

---

[2] The arrangement uses a distributed analysis emphasizing the underlying characteristics of a DoS attack, i.e., congestion and slow server response, to produce a robust and comprehensive DoS solution. Thus, this architecture 10 can stop new attacks rather than some solutions that can only stop previously seen attacks. Furthermore, the distributed architecture 10 will frequently stop an attack near its source, before it uses bandwidth on the wider Internet 14 or congests access links to the targeted victim 12. (Appellant's specification page 6, lines 9-18).

[3] Therefore there exists a need for a system and method allowing for the distributed state of a network, such as information about attack traffic, to be quickly and accurately collected. A system and method are needed for quickly and accurately diagnosing network attacks by determining information such as the source of, or a partial path of, attack traffic. (Yavatkar Col. 2, lines 44-51).

The system and method of an exemplary embodiment of the present invention use agents--mobile software modules--to collect data on the state of a network during a network attack, allowing for more accurate diagnosis of an attack. During a network attack, the system and method of the present invention allow for details on the attack traffic (e.g., the source of the attack traffic and path of the attack traffic) to be gathered. The source of the attack traffic may be the originator of the attack traffic or, for example a gateway allowing attack traffic to enter a network and which is, in effect, the source of attack traffic to the network. Such information then may be used to halt the attack or insulate the network from the attack. (Yavatkar Col. 3, lines 25-37).

"agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node)."[4]

Appellant contends that Yavatkar fails to disclose whether at (col. 3 line 65 - col. 4, line 23) or elsewhere the feature of sending queries to request the statistical information as recited in claim 1. At col. 3 line 65 - col. 4, line 23, Yavatkar discloses:

> **In an exemplary embodiment of the present invention, a watchdog agent monitors the node on which it operates for traffic having characteristics of a network attack. A watchdog agent may also monitor for and detect a network attack at a device other than the device on which it operates. On detecting an attack the watchdog agent launches one or more bloodhound agents to trace the attack traffic. The watchdog agent launches various types of bloodhound agents based on the type of attack detected; each bloodhound agent is designed to trace traffic from one type of attack. In an exemplary embodiment a bloodhound agent moves across the network, tracing the path or paths taken by attack traffic. To trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found. After gathering such information a bloodhound agent reports to the watchdog agent, which, in turn, may report to a human operator or, possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects.**

---

[4] See examiner's action pages 2-3.

The examiner has not used the teaching from the background of Yavatkar. (Col. 1, line 65 to Col. 2, line 23), set forth below:

> Systems exist for collecting information about network traffic. For example, to determine the node which is the source of attack traffic (or the gateway allowing such traffic into a network, which in such a case may be considered a source) and the path or paths taken by such traffic, a human operator may access each link at a node receiving such traffic and analyze the incoming traffic using a sniffer. A sniffer is a device which may record network statistics at a node. The operator may identify which of the physical links attached to the node is receiving a certain type or amount of traffic and then move to the node on the other end of the identified link. The path or paths of traffic from the source of the traffic may be found by traversing the network from node to node, using the sniffer at each node in a path, until the source is reached. Such a diagnosis is slow and inaccurate. A similar analysis may be performed from a central console which may query remote nodes for information about the source of incoming traffic. Such a diagnosis is also slow and inaccurate, as it requires commands to nodes and responses from nodes to be transmitted across the network. The speed at which attacks occur and the speed at which such problems must be fixed makes such detection methods ineffective. A path taken by traffic may be described as the equipment traversed by traffic as the traffic crosses a network or networks (e.g., a series of nodes and links, or a series of sub-networks).

Appellant contends that the sniffer approach described by Yavatkar does not anticipate Appellant's claims either since *inter alia* the sniffer approach does not involve sending of queries or processing of the statistical information received in response to the sent queries.

Yavatkar fails to disclose the feature of sending queries … to request the statistical information, as recited in claim 1. Nowhere in the cited passage does Yavatkar suggest much less describe statistical information on network packets sent over the network. Yavatkar describes a watchdog agent that monitors for traffic having characteristics of a network attack.

Yavatkar does not disclose that it collects statistical information on network packet traffic. In the instant case the reference is devoid of any discussion of sending queries … to request the statistical information collected by data collectors.

Claim 1 also requires sending queries to data collectors. However, Yavatkar describes that the bloodhound agents "self destruct." Thus, the watchdog and bloodhound agents are not described in a manner in which the watchdog queries the bloodhound agents. Indeed, once a bloodhound agent sends its report, it self-destructs, which in Appellant's opinion, making it difficult for the bloodhound agent to respond to queries.

Yavatkar does not describe that the bloodhound agents are responsive to queries and in particular queries for statistical information. Rather, Yavatkar is directed to a process in which bloodhound agents are instantiated node to node in an attempt to trace the path of an attack.

Claim 1 further distinguishes since Yavatkar fails to disclose: "processing the statistical information to determine the source of suspicious network traffic sent to the data center." The examiner contends that this feature is described by Yavatkar at col. 3, lines 25-37 and col. 18, lines 32-53, which passages are reproduced below:

> **The system and method of an exemplary embodiment of the present invention use agents--mobile software modules--to collect data on the state of a network during a network attack, allowing for more accurate diagnosis of an attack. During a network attack, the system and method of the present invention allow for details on the attack traffic (e.g., the source of the attack traffic and path of the attack traffic) to be gathered. The source of the attack traffic may be the originator of the attack traffic or, for example a gateway allowing attack traffic to enter a network and which is, in effect, the source of attack traffic to the network. Such information then may be used to halt the attack or insulate the network from the attack. (Yavatkar col. 3, lines 25-37)**
>
> **To report, the bloodhound agent moves across the network to the node of its launch point and provides its findings to the watchdog agent. The bloodhound agent transmits the data it has collected to the watchdog agent using a messaging service. After reporting, the bloodhound agent is destroyed. In an exemplary embodiment, the bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. The path as described by the bloodhound agent comprises links**

> **and nodes. Links may be denoted using pairs of port/node combinations. For example, a link may be denoted as the link connecting port "Interface 2" on node 22.49.1.3 to port "Interface 4" on node 22.49.1.7. In alternate embodiments the findings may include other types of information. In an alternate embodiment the bloodhound agent need not move to its launch point to report its findings; for example, it may transmit the information across the network using a messaging service and then self-destruct. (Yavatkar col. 18, lines 32-53)**

The examiner equates the data collectors to the bloodhound agents described by Yavatkar.[5] While the bloodhound agents provide findings to the watchdog agent, and transmit a report, Yavatkar describes the report indicating "the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic." Yavatkar also describes: "The path as described by the bloodhound agent comprises links and nodes. Links may be denoted using pairs of port/node combinations." None of this is seen to be statistical information that is used to determine the source of an attack. Rather, Yavatkar merely describes a well-known path tracing scheme, in which the bloodhound agents are deployed along paths that are supposedly part of the attack.

In response to Appellant's argument, the examiner argues that the examiner is entitled to give terms in Appellant's claims their broadest reasonable interpretation, and proceeds to equate "sending queries" to "launching bloodhound agents" and "collecting statistical information on network packets sent over the network" to "gathered information."

Appellant contends that the Examiner improperly ignores Appellant's specification to guide the examiner to give the claims their broadest reasonable construction. The Federal Circuit in *In re Morris*[6] requires the examiner to apply the Court's guidance on what "reasonable" means:

> Since it would be unreasonable for the PTO to ignore any interpretive guidance afforded by the applicant's written description, either phrasing connotes the same notion: as an initial matter, the PTO applies to the verbiage of the proposed claims the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, *taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written*

---

[5] "agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node" (Office action page 3)
[6] *In re Morris*, 127 F.3d 1048 (Fed. Cir. 1997).

> *description* contained in the applicant's specification." [emphasis supplied]

According to *Morris,* the examiner must apply the broadest reasonable meaning to terms "in their ordinary usage as they would be understood by one of ordinary skill in the art." The examiner has not provided any rational basis upon which one of ordinary skill in the art would construe "sending queries to data collectors" as the same as launching bloodhound agents based on the type of attack detected or construing "statistical information on network packets" as "gathered information." For example, the examiner states: "The gathered information is equated to the statistical information because the claim language merely recites statistical information and does not specify the type of statistical information that is collected."

The examiner errs, since claim 1 does specify the type of statistical information collected, namely, statistical information on network packets. Had Yavatkar described collecting statistical information, then Appellant would have narrowed the scope of "statistical information." However, Yavatkar, in fact, fails to describe "statistical information on network packets," and thus all that Appellant needs to distinguish this feature over Yavatkar is the act of "collecting statistical information on network packets."

Rather, Yavatkar describes gathering information as: "gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process." [Yavatkar Col. 2, line 56].

Yavatkar also discloses: "In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found. Thus, Yavatkar teaches that the bloodhound agents trace the path of the attack. After gathering such path information a bloodhound agent reports to the watchdog agent. [Yavatkar Col. 4, line 16].

In *Morris*, the specification lacked any text to guide the Examiner in construing what the disputed claim term meant. Based on the absence of any such text, the Court stated that the Examiner's interpretation was reasonable:

> Absent an express definition in their specification, the fact that appellants can point to definitions or usages that conform to their interpretation does not make the PTO's definition unreasonable when the PTO can point to other sources that support its interpretation."

In the present application, the written description discusses querying data collectors and statistical information on network packets in great detail. There is no ambiguity, as there was in *Morris*. Therefore, by construing querying data collectors and collecting statistical information with totally unrelated concepts, the examiner improperly ignores the meaning that these features have in Appellant's specification and improperly conflates them with unrelated teachings such as "launching bloodhound agents" and "gathering information" disclosed by Yavatkar.

Appellant does not ask the examiner to read limitations into the claims, as was the case in *In re Van Geuns*[7]. In *Van Geuns*, the specification disclosed a magnet assembly used for NMR. The claim, however, recited a magnet assembly that provided a uniform magnetic field, with no mention of NMR. The cited reference disclosed a magnet assembly that generated a relatively uniform field. *Van Geuns* is inapplicable to the present case, because the claim elements, e.g., querying data collectors and collecting statistical information are expressly defined in the specification and positively recited in the claims.

Appellant's claims recite particular features and the examiner must find those features in the prior art, rather than conflate them with non-relevant teachings. Therefore, the specification is available to help the examiner understand these features and the examiner may properly review the specification in construing a claim term. In the present case, the Examiner is attempting to construe these features without the benefit of the guidance offered by Applicant's specification.

In response to Appellant's argument made in Reply to the final action, the examiner stated:

> **After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a second request is not needed. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the currently claimed limitations.**

---

[7] *In re Van Geuns*, 988 F.2d 1181 (Fed. Cir. 1993).

Appellant contends that according to Yavatkar, the bloodhound agents work in a different manner, as discussed in Reply to the final action.[8] Moreover, even if the examiner's interpretation of how Yavatkar works is correct, this interpretation fails to address the features of "sending queries to data collectors" or "sending the statistical information from the data collectors in response to the queries" or "the queries to request the statistical information"

Therefore, claim 1 is allowable over Yavatkar since "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983) and Yavatkar fails to disclose the features of sending queries to data collectors… that … collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors … and processing the statistical information to determine the source of suspicious network traffic sent to the data center.

Claim 2

Claim 2 adds the feature of sending queries to the data collectors for the statistical information based on victim destination address.

The examiner contends these features are disclosed in Yavatkar, at (col. 13, lines 44-53 and col. 3, line 65 - col. 4, line 23. These passages from Yavatkar are reproduced below:

> **In an exemplary embodiment of the present invention, a watchdog agent monitors the node on which it operates for traffic having characteristics of a network attack. A watchdog agent may also monitor for and detect a network attack at a device other than the device on which it operates. On detecting an attack the watchdog agent launches one or more bloodhound agents to trace the attack traffic. The watchdog agent launches various types of bloodhound agents based on the type of attack detected; each bloodhound agent is designed to trace traffic from one type of attack. In an exemplary embodiment a bloodhound agent moves across the network, tracing the path or paths taken by attack traffic. To trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found. After gathering such information a bloodhound agent reports to the watchdog agent, which, in turn, may report to a human operator or, possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects. [Yavatkar, col. 13, lines 44-53].**

[8] Amendment In Reply To Action Of June 14, 2006 pages 12-13.

> **If the source of the attack traffic messages can be identified (by, for example, its IP address) the source can be shut down or disabled. For example, the Internet provider allowing the source device access to the Internet may be notified and may terminate the source device's Internet access. However, through the use of IP spoofing the source of the attack may be obscured. Using IP spoofing the TCP/IP packets constituting the attack traffic indicate a source which is not the actual source device--the sender of the attack traffic inserts a false "return address." [Yavatkar, col. 3, line 65 - col. 4, line 23].**

One skilled in the art would not recognize from these passages or elsewhere in Yavatkar, the features of claim 2. Yavatkar does not describe that statistical information based on victim destination address is sent from the data collectors or that Yavatkar describes sending queries to the data collectors. Yavatkar discloses that the bloodhound agents report to the watchdog agents, which may report to a human operator. However, the report is of the path taken by the attack not statistical information. Yavatkar does not describe that the report is sent in response to a query from the watchdog agent or that statistical information sent is based on victim[9] destination address. Rather, the report is sent prior to the bloodhound agent self-destructing.

Claim 3

The examiner contends that Yavatkar discloses: "Determining, from at least in part, the collected statistical information, what data centers are involved in the attack on the victim data center (col. 8, lines 32-53, the agents determine the source of the attack and other nodes that it affected)."

In rejection of Claim 3, the examiner improperly conflates "statistical information collected on network packets that traverse the network," with the path information collected by Yavatkar. The examiner has not shown that Yavatkar inherently possesses the claimed statistical information.

Claims 4 and 5

For the purposes of this appeal only, Claims 4 and 5 stand or fall together. Claim 4 is representative of this group of claims.

---

[9] In response to the final rejection Appellant had sought to clarify this term, since during prosecution it was inadvertently left in the claim and no longer had strict antecedent basis. However, it is clear on the record that the term refers to the data center.

Claim 4 distinguishes over Yavatkar since Yavatkar neither describes nor suggests that determining is performed by a control center that receives the statistical information from the data collectors and includes sending data to/from a gateway device that is associated with the victim data center.

In Yavatkar the watchdog agent does not analyze traffic to determine the source, the analysis is performed by the bloodhound agents[10] indeed the watchdog agent creates[11] the bloodhound agents and indeed the watchdog may not even be needed.[12] Rather, than analyzing to determine the source, the watchdog is provided to monitor[13] and launch[14] bloodhound agents and report to an operator.[15]

Accordingly claim 4 is allowable over Yavatkar since Yavatkar does not describe all elements of a claimed invention arranged as in the claim *Connell* supra.

Claim 6

Claim 6 requires that the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control center in response to the queries sent from the central control center.

The examiner does not explicitly address this feature and instead merely points Appellant to Fig. 3. Fig. 3 is reproduced below:

---

[10] On detecting network attack, a watchdog agent creates a second type of agent, a bloodhound agent, which analyzes attack traffic by moving through the network and gathering information. The watchdog agent remains stationary.

[11] Id.

[12] In an alternate embodiment, a stationary watchdog agent may not be needed; a bloodhound agent may collect data without the prompting or direction of such a watchdog agent. Furthermore, the watchdog agent may exist as a process other than an agent; for example, a process functioning as a does a watchdog agent may be a C++ application

[13] In an exemplary embodiment of the present invention, a watchdog agent monitors the node on which it operates for traffic having characteristics of a network attack.

[14] The watchdog agent launches various types of bloodhound agents based on the type of attack detected.

[15] After gathering such information a bloodhound agent reports to the watchdog agent, which, in turn, may report to a human operator or, possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects.

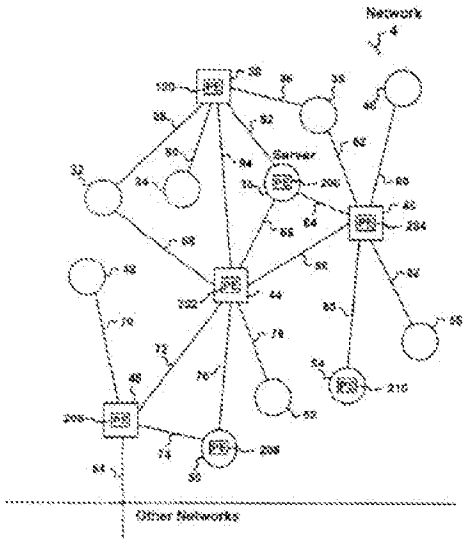

Figure 3

Yavatkar's Fig. 3 merely shows a network with nodes and links. Yavatkar does not describe a redundant network that does not carry the network traffic, to carry the statistical information in response to queries to the control center. Accordingly, Yavatkar neither anticipates nor renders obvious claim 6.

Claim 9

Claim 9 recites that if a source of the attack is behind a gateway, the control center issues a request to the gateway that the attacking system is behind to prevent the attacking traffic … from reaching the network.

Yavatkar describes "After gathering such information a bloodhound agent reports to the watchdog agent, which in turn, may report to a human operator or, possibly, attempt to halt the attack." However, Yavatkar fails to describe that the bloodhound will issue a request to a gateway. Yavatkar mentions that in respond mode, the watchdog agent may attempt to halt the attack by either launching an agent which alters routing tables or altering the routing tables itself. Yavatkar also describes launching an agent which functions as a firewall or installing filters, report findings, communicate with network administrators so that the network administrator may

use the findings to cure the problem.[16] In no event does Yavatkar describe that the watchdog, which the examiner analogized to the control center of claim 9, contacts the gateway.

Claim 15

Claim 15 adds the feature of receiving from a gateway … a notification that the victim is under attack. For the reasons discussed in claim 1, the combination of this feature with the features of sending queries to data collectors … that … collect statistical information on network packets … and determining the data center(s) … involved in the attack … by analyzing collected statistical information from the data collectors, makes this claim allowable over Yavatkar.

In addition, Yavatkar does not describe: "the queries being requests for statistical information from data collectors that have examined network traffic with the victim destination address … ." Yavatkar does not make queries and does not make queries to data collectors that have examined network traffic with the victim destination address. Rather, upon detection of an attack by the watchdog agent, it launches the bloodhounds that trace the path of attacking traffic. No queries based on victim destination addresses are sent to the bloodhound agents by the watchdog agent.

Claim 16

Claim 16 requires … communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center. Yavatkar does not describe communicating statistical information, and in particular, communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center.

---

[16] After a response from the bloodhound agent the watchdog agent transitions to the respond mode. In the respond mode the watchdog agent may attempt to halt the attack. For example the watchdog agent may launch an agent which alters routing tables to prohibit traffic from a given source from entering the network, or may perform such an operation itself The watchdog agent may launch an agent which functions as a firewall; such an agent moves to the point in the network which is the ingress point for attack traffic. The watchdog agent may install several intermediate filters in the network which prevent attack traffic from being forwarded. The watchdog agent may report findings (e.g., the source of the attack; the path or paths taken by attack traffic) to a network administrator. In an exemplary embodiment the watchdog agent communicates with network administrators via a management console application; alternate embodiments may use other methods. The network administrator may use the findings to cure the problem. After attempting to halt the attack or contact an administrator the watchdog agent transitions to the monitoring mode.

Claim 17

For analogous reasons, as in claim 9, claim 17 is not described by Yavatkar since the reference does not describe that … the control center issues a request to the gateway to block the attacking traffic.

Claims 20, 21 and 26-28

For the purposes of this appeal only, Claims 20, 21 and 26-28 stand or fall together. Claim 20 is representative of this group of claims.

Claim 20 is directed to a system to thwart denial of service attacks. Claim 20 distinguishes over Yavatkar since Yavatkar neither describes nor suggests a plurality of monitors dispersed …collecting statistical data on network traffic, a control center coupled to the plurality of data collectors, the control center executing a computer program product … comprising instructions … to receive … a notification … and in response to receiving the notification send queries to data collectors to request the statistical information from the data collectors, the statistical information used to determine the source of suspicious network traffic … and a gateway device … disposed to protect the … data center, and … coupled to the control center.

Claim 20 is directed to a system including a plurality of monitors that collect statistical information on network traffic, which are queried by a control center in response to a notification that the data center is under attack.

Yavatkar does not describe such an arrangement. Rather, in Yavatkar in response to a notification of an attack a watchdog agent deploys bloodhound agents, which report on paths from an attack and then self-destruct. Yavatkar does not describe the bloodhound agents, as collecting statistical information. Nor does Yavatkar describe that the bloodhound agents are queried by the watchdog or that the watchdog sends queries. The bloodhound agents do not persist, but rather self destruct and hence cannot meet the limitation of the monitors, since the monitors are required to be coupled to the control center and respond to queries from the control center.

Claim 22

Claim 22 is not described by Yavatkar, since Yavatkar does not describe that the control center further comprises instructions to determine a source of the attack on the victim data center by analyzing collected statistical information from the data collectors.

According to Yavatkar the bloodhound agents trace an attack. No mention, however, is made in Yavatkar of analysis by the control center of any information, in particular, statistical information to determine the source of an attack.

Claim 23

Yavatkar does not describe that the control center and gateway device associated with the victim data center exchange data including statistical information to thwart the attack.

Claim 24

Yavatkar does not describe that the data exchanged between the control center and gateway device … are sent over a redundant network that is a different network than the network that is being monitored by the data collectors. The examiner has not shown that in Fig. 3 of Yavatkar a separate network that does not carry the monitor traffic is used to communicate between the bloodhound and watchdog agents.

Claim 25

Claim 25 is allowable for analogous reasons as given for claim 9.

Claims 29 and 32

For the purposes of this appeal only, Claims 29 and 32 stand or fall together. Claim 32 is representative of this group of claims.

Claim 29 is directed to a computer program product … for protecting a victim data center against a denial of service attack …comprising instructions to … send queries to data collectors … that … sample network traffic and collect statistical information on packets sent over the network, the queries to request statistical information from data collectors that have examined network traffic with the victim destination address and determine a source of the attack on the victim data center by analyzing collected information from the data collectors.

Yavatkar does not describe such an arrangement. Yavatkar describes a watchdog agent that deploys bloodhound agents that report on paths involved in an attack and then self-destruct. The watchdog agent does not send queries to the data collectors that collect statistical information nor that can respond to the queries based on the victim destination address. Yavatkar does not describe any process that determines a source of the attack based on analysis of the collected statistical information. Rather, in Yavatkar the analysis is based on paths identified by the bloodhound agents, before the bloodhound agents self-destruct.

Claim 30

Claim 30 requires instructions to: "send data including statistical information between a gateway device that is disposed with the victim data center and a control center." Claim 30 is allowable for analogous reasons as given for claim 16.

Claim 31

Claim 31 is allowable for analogous reasons as given for claim 9.

2. Yavatkar et al., '702 in view of Hill et al. '804 fail to render obvious Claims 13 and 14.

Claims 13 and 14

Each of claims 13 and 14 are allowable at least because of the features recited in claim 1, since Yavatkar does not anticipate claim 1 and Hill does not cure the deficiencies in Yavatkar as noted in the above argument. Further, the examiner uses Hill to teach "classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2 lines 53-60; col. 6 lines 9-22)." Appellant notes that the teachings in Hill are directed to attack simulation, not to an actual attack or a system to detect and thwart an attack.

Conclusion

Appellant submits that Claims 1-33 are patentable over the cited art. Therefore, the Examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: 3/19/03

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

Appendix of Claims

1. A method of protecting a data center against a denial of service attack, the method comprises:

sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors; and

sending the statistical information from the data collectors in response to the queries; and

processing the statistical information to determine the source of suspicious network traffic sent to the data center.

2. The method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for the statistical information based on victim destination address.

3. The method of claim 1 wherein processing further comprises:

determining, from at least in part, the collected statistical information, what data centers are involved in the attack on the victim data center.

4. The method of claim 3 wherein determining is performed by a control center that receives the statistical information from the data collectors, and determining further comprises:

sending data to/from a gateway device that is associated with the victim data center.

5. The method of claim 4 wherein the gateway identifies the network address of the victim, via a message to the control center.

6. The method of claim 1 wherein the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control center in response to the queries sent from the central control center.

7. The method of claim 5 wherein message indicates the type of attack.

8. The method of claim 1 wherein a source of the attack is behind a gateway.

9. The method of claim 8 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway that the attacking system is behind to prevent the attacking traffic from attacking system from reaching the network.

10. The method of claim 8 wherein if a source of the attack is behind a gateway, the gateway that the attacking system is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address.

11. The method of claim 1 wherein if a source of the attack is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attacking system.

12. The method of claim 1 wherein if a source of the attack is not behind a gateway, the method further comprises:

contacting administrators at locations involved in the attack to have the administrators take action to filter out packets with the destination address.

13. The method of claim 1 wherein the attack is a low-grade spoofing-type of attack that does not compromise network traffic flow between the victim data center and Internet.

14. The method of claim 1 wherein the attack is a high-grade attack that compromises network traffic flow between the victim data center and Internet.

15. A method of protecting a victim data center against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses;

receiving, from a gateway disposed near the victim data center, a notification that the victim data center is under an attack;

sending queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network packets and collect statistical information on network packets sent over the network, the queries being requests for statistical information from data collectors that have examined network traffic with the victim destination address; and

determining the data center or centers involved in the attack on the victim data center by analyzing collected statistical information from the data collectors.

16. The method of claim 15 further comprising:

communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center.

17. The method of claim 16 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway to block the attacking traffic.

18. The method of claim 17 wherein if a source of the attack is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address.

19. The method of claim 15 wherein if a source of the attack is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address.

20. A system to thwart denial of service attacks on a victim data center, the system comprising:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic;

a control center coupled to the plurality of data collectors, the control center executing a computer program product stored on a computer readable medium, comprising instructions for causing a computer to:

receive from the victim site a notification that the victim data center is under an attack; and in response to receiving the notification,

send queries to data collectors to request the statistical information from the data collectors, the statistical information used to determine the source of suspicious network traffic being sent to the victim;

a gateway device that passes network packets between the network and the victim data center, the gateway disposed to protect the victim data center, and being coupled to the control center.

21. The system of claim 20 wherein the data collectors collect statistical information on network packets that pass through points in the network that the data collectors monitor.

22. The system of claim 20 wherein the control center further comprises instructions to:

determine a source of the attack on the victim data center by analyzing collected statistical information from the data collectors.

23. The system of claim 20 wherein the control center and gateway device associated with the victim data center exchange data including statistical information to thwart the attack.

24. The system of claim 20 wherein data exchanged between the control center and gateway device associated with the victim data center are sent over a redundant network that is a different network than the network that is being monitored by the data collectors.

25. The system of claim 20 wherein if the control center determines that the source of the attack is behind a gateway, the control center issues a request to the gateway that the source of the attack is behind to block the attacking traffic.

26. The system of claim 20 wherein if the control center determines that the source of the attack is behind a gateway, the control center issues a request to the gateway to selectively discard traffic that contains the victim destination address.

27. The system of claim 20 wherein if the source of the attack is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the source of the attack.

28. The system of claim 27 wherein if the source of the attack is not behind a gateway, the system includes instructions to contact administrators at locations involved in attack to have the administrators take action to filter out packets with the victim destination address.

29. A computer program product residing on a computer readable media for protecting a victim data center against a denial of service attack, the computer program product, comprising instructions for causing a computing device to:

receive a notification that the victim data center is under an attack;

send queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network traffic and collect statistical information on packets sent over the network, the queries to request statistical information from data collectors that have examined network traffic with the victim destination address; and

determine a source of the attack on the victim data center by analyzing collected information from the data collectors.

30. The computer program product of claim 29 further comprising instructions to:

send data including statistical information between a gateway device that is disposed with the victim data center and a control center.

31. The computer program product of claim 29 further comprising instructions to:

determine whether the source of the attack is behind a gateway and if the source of the attack is behind a gateway,

issue a request to the gateway to block the attacking traffic.

32. The computer program product of claim 29 further comprising instructions to:

determine whether the source of the attack is behind a gateway and if the source of the attack is not behind a gateway,

send a message to contact administrators at locations involved in the attack to filter out packets having the destination address.

33. The method of claim 1 further comprising:

receiving from the victim site a notification that the victim site is under an attack.

Evidence Appendix

None

Related Proceedings Appendix

None